

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

SEMESTRÁLNÍ PRÁCE



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

**FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ**

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

**APLIKACE PRO GENEROVÁNÍ A OVĚŘOVÁNÍ
KONFIGURACÍ SÍŤOVÝCH ZAŘÍZENÍ**

APPLICATION GENERATING AND VERIFYING CONFIGURATIONS OF NETWORK DEVICES

SEMESTRÁLNÍ PRÁCE

SEMESTRAL THESIS

AUTOR PRÁCE

AUTHOR

Bc. Juraj Korček

VEDOUCÍ PRÁCE

SUPERVISOR

doc. Ing. Jan Jeřábek, Ph.D.

BRNO 2019

Semestrální práce

magisterský navazující studijní obor **Informační bezpečnost**

Ústav telekomunikací

Student: Bc. Juraj Korček

ID: 187238

Ročník: 2

Akademický rok: 2019/20

NÁZEV TÉMATU:

Aplikace pro generování a ověřování konfigurací síťových zařízení

POKyny PRO VYPRACOVÁNÍ:

Seznamte se s problematikou síťových zařízení, síťových operačních systémů, hlavních používaných komunikačních protokolů a způsobů konfigurace těchto zařízení. Dále prostudujte problematiku osvědčených postupů konfigurace, zejména s ohledem na bezpečnost fungování zařízení v síti a také problematiku anonymizace těchto konfigurací. Navrhněte systém či aplikaci, která bude umět pro vybranou množinu síťových zařízení vytvářet přednastavené parametry nastavení, které bude možné na dané síťové zařízení aplikovat. Dále musí daná aplikace umět verifikovat správnost existujících konfigurací, upozornit na případné nedostatky a i konfiguraci modifikovat tak, aby splňovala hlavní bezpečnostní a provozní standardy a doporučení. Fungování aplikace ověřte na testovacích vzorcích síťových konfigurací různých zařízení z několika různých sítí a případně i různých výrobců.

V rámci semestrálního projektu je třeba vypracovat teoretickou část zadání, vybrat vhodné programovací prostředí pro plánovanou aplikaci a navrhnout a popsat strukturu dané aplikace či systému, včetně základního popisu jednotlivých komponent a jejich předpokládané funkcionality. Vlastní řešení mírně rozpracujte.

DOPORUČENÁ LITERATURA:

[1] Stallings W., Network security essentials: applications and standards. 6th ed. Hoboken: Pearson education, 2017, 445 s. ISBN 978-0-13-452733-8.

[2] McMillan, T., CCNA Security Study Guide: Exam 210-260. 2nd ed. USA: Sybex, 2018, 384 s. ISBN 978-1--1-940993-9.

Termín zadání: 23.9.2019

Termín odevzdání: 21.12.2019

Vedoucí práce: doc. Ing. Jan Jeřábek, Ph.D.

Konzultant:

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

UPOZORNĚNÍ:

Autor semestrální práce nesmí při vytváření semestrální práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

VYHLÁSENIE

Vyhlasujem, že svoju semestrálnú prácu na tému „Applikace pro generování a ověřování konfigurací síťových zařízení“ som vypracoval samostatne pod vedením vedúceho semestrálnej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej semestrálnej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto semestrálnej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno

.....

podpis autora

Obsah

Úvod	15
Záver	17
Literatúra	19
Zoznam symbolov, veličín a skratiek	23
Zoznam príloh	25
A Zdrojové súbory	27
A.1 Konfiguračné súbory	27
B Checklist	29

Zoznam obrázkov

Zoznam tabuliek

Zoznam výpisov

Úvod

Kybernetická bezpečnosť je bezpochyby jednou z hlavných tém 21. storočia. Útoky na infraštruktúru a systémy naberajú nielen na frekvencii, ale čo je ešte horšie na sofistikovanosti. Napriek častému zdôrazňovaniu odborníkov o kladenie čoraz väčšieho dôrazu na bezpečnosť pri návrhu, implementácii a nasadení, sa stále stretávame s fatálnymi dôsledkami, ktoré boli spôsobené nedostatočným venovaním pozornosti bezpečnosti.

Problém nedostatočného zabezpečenia nie je ani tak nevedomosť základných bezpečnostných praktík administrátorov alebo programátorov, ale potreba rýchleho nasadenia systému a infraštruktúry s odložením implementácie bezpečnostných praktík na neskôr. Tieto problémy vznikajú aj pri dodatočnej implementácii nových modulov a pridaní novej infraštruktúry, kedy sa nemení celok, ale pridanie jednej časti môže výrazne ovplyvniť a zmeniť stav bezpečnosti celého systému. Z tohto dôvodu je priam žiadúce disponovať nejakým procesom alebo nástrojom na dodatočné zistenie nedostatkov a ich následnú elimináciu. Veľmi silnou motiváciou by malo byť aj to, že dôsledkom bezpečnostných nedostatkov sú globálne miliardové škody a straty reputácií firiem.

Jednou z hlavných častí infraštruktúry, kde dochádza k významným bezpečnostným incidentom je počítačová sieť, bez ktorej by dnes informačné technológie nevedeli fungovať. Preto sa táto práca bude zaoberať práve ňou, keďže je vstupnou bránou do systémov a jej vyradením alebo zneužitím prichádzajú organizácie o finančné prostriedky, citlivé dáta a dôveru užívateľov.

Výsledkom tejto práce bude aplikácia overujúca nastavenia sieťových zariadení prevažne v lokálnej sieti, ktorá umožňuje zjednať nápravu na základe nájdených nedostatkov. Výhodou oproti existujúcim riešeniam bude otvorenosť kódu a modularita, ktorá umožní rozšírenie aplikácie na sieťové zariadenia rôznych výrobcov. Dôležitým výstupom bude taktiež zoznam bezpečnostných a prevádzkových odporúčaní vychádzajúcich z rôznych štandardov a odporúčaní, ktoré môžu byť v budúcnosti použité ďalšími užívateľmi aplikácie pri zostavovaní modulov pre zariadenia rôznych výrobcov. Jednou z kľúčových vlastností je bezplatnosť, keďže podľa zistení polovica útokov smeruje na malé firmy, ktoré bezpečnosť často neriešia z finančnej náročnosti programov na detekciu bezpečnostných nedostatkov.

Záver

Zhrnutie práce.

Literatúra

- [1] ALSADEH, Ahmad. Augmented SEND: Aligning Security, Privacy, and Usability. In: *RIPE NCC* [online]. 12.5.2015 [cit. 2019-11-02]. Dostupné z: <https://ripe70.ripe.net/presentations/67-RIPE70-SEND.pdf>
- [2] PODERMAŇSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: zkrocení zlých směrovačů. In: *ROOT.CZ* [online]. 12.2.2015 [cit. 2019-11-02]. Dostupné z: <https://www.root.cz/clanky/bezpecne-ipv6-zkroceni-zlych-smerovacu/>
- [3] KHANDELWAL, Manjul. OSPF Security: Attacks and Defenses. In: *SANOG* [online]. 2016 [cit. 2019-11-04]. Dostupné z: https://www.sanog.org/resources/sanog28/SANOG28-Tutorial_OSPF-Security-Attacks-and-Defences-Manjul.pdf
- [4] PODERMAŇSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: když dojde keš — obrana. In: *ROOT.CZ* [online]. 19.3.2015 [cit. 2019-11-02]. Dostupné z: <https://www.root.cz/clanky/bezpecne-ipv6-kdyz-dojde-kes-obrana/>
- [5] PODERMAŇSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: když dojde keš. In: *ROOT.CZ* [online]. 12.3.2015 [cit. 2019-11-02]. Dostupné z: <https://www.root.cz/clanky/bezpecne-ipv6-kdyz-dojde-kes/>
- [6] PODERMAŇSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: trable s multicastem. In: *ROOT.CZ* [online]. 5.3.2015 [cit. 2019-11-02]. Dostupné z: <https://www.root.cz/clanky/bezpecne-ipv6-trable-s-multicastem/>
- [7] GRÉGR, Matěj a Tomáš PODERMAŇSKI. Bezpečné IPv6: vícehlavý útočník. In: *ROOT.CZ* [online]. 26.2.2015 [cit. 2019-11-02]. Dostupné z: <https://www.root.cz/clanky/bezpecne-ipv6-vicehlavy-utocnik/>
- [8] PODERMAŇSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: trable s hlavičkami. In: *ROOT.CZ* [online]. 19.2.2015 [cit. 2019-11-02]. Dostupné z: <https://www.root.cz/clanky/bezpecne-ipv6-trable-s-hlavickami/>
- [9] GRÉGR, Matěj a Tomáš PODERMAŇSKI. Bezpečné IPv6 : směrovač se hlásí. In: *ROOT.CZ* [online]. 5.2.2015 [cit. 2019-11-02]. Dostupné z: <https://www.root.cz/clanky/bezpecne-ipv6-smerovac-se-hlasi/>
- [10] IPv6 First-Hop Security Configuration Guide. In: *Cisco* [online]. San Jose [cit. 2019-11-02]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-1sg/ipv6-15-1sg-book.pdf

- [11] BOUŠKA, Petr. *Cisco IOS 12 - IEEE 802.1x a pokročilejší funkce* [online]. In: . 2007 [cit. 2019-11-02]. Dostupné z: <https://www.samuraj-cz.com/clanek/cisco-ios-12-ieee-802-1x-a-pokrocilejsi-funkce/>
- [12] MOLENAAR, René. Cisco IOS features that you should disable or restrict. In: *NetworkLessons.com* [online]. [cit. 2019-11-02]. Dostupné z: <https://networklessons.com/uncategorized/cisco-ios-features-that-you-should-disable-or-restrict>
- [13] BOUŠKA, Petr. Cisco IOS 23 - Autentizace uživatele na switchi vůči Active Directory. In: *SAMURAJ-cz* [online]. 2009 [cit. 2019-11-02]. Dostupné z: <https://www.samuraj-cz.com/clanek/cisco-ios-23-autentizace-uzivatele-na-switchi-vuci-active-directory/>
- [14] BARKER, Elaine a Allen ROGINSKY. Transitioning the Use of Cryptographic Algorithms and Key Lengths. In: *NIST* [online]. 2019 [cit. 2019-11-02]. Dostupné z: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf>
- [15] VYNCKE, Erik. ND on wireless links and/or with sleeping nodes. In: *IETF* [online]. [cit. 2019-11-02]. Dostupné z: <https://www.ietf.org/proceedings/89/slides/slides-89-v6ops-3.pdf>
- [16] CIS Cisco IOS 15 Benchmark. In: *Center For Internet Security* [online]. 2015 [cit. 2019-11-02]. Dostupné z: <https://www.cisecurity.org/benchmark/cisco/>
- [17] SINGH, Shashank. Cisco Guide to Harden Cisco IOS Devices. In: *Cisco* [online]. 2018 [cit. 2019-11-02]. Dostupné z: <https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>
- [18] GRAESSER, Dana. Cisco Router Hardening Step-by-Step. In: *SANS Institute* [online]. 2001 [cit. 2019-11-02]. Dostupné z: <https://www.sans.org/reading-room/whitepapers/firewalls/paper/794>
- [19] PILIHANTO, Atik. A Complete Guide on IPv6 Attack and Defense. In: *SANS Institute* [online]. SANS Institute, 2012 [cit. 2019-11-02]. Dostupné z: <https://www.sans.org/reading-room/whitepapers/detection/paper/33904>
- [20] REY, Enno, Antonios ATLASIS a Jayson SALAZAR. MLD Considered Harmful. In: *RIPE NCC* [online]. 2016 [cit. 2019-11-02]. Dostupné z: https://ripe72.ripe.net/presentations/74-ERNW_RIPE72_MLD_Considered_Harmful_v1_light_web.pdf

- [21] VYNCKE, Erik. IPv6 First Hop Security: the IPv6 version of DHCP snooping and dynamic ARP inspection. In: *Slidde Share* [online]. 2012 [cit. 2019-11-02]. Dostupné z: <https://www.slideshare.net/IKTNorge/eric-vyncke-layer2-security-ipv6-norway>
- [22] IPv6 First-Hop Security Configuration Guide. In: *Cisco* [online]. 2012 [cit. 2019-11-02]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-s/ip6f-15-s-book/ip6-snooping.html
- [23] GREGR, Matej, Petr MATOUSEK, Miroslav SVEDA a Tomas PODERMANSKI. Practical IPv6 monitoring-challenges and techniques. In: *12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011) and Workshops*. IEEE, 2011, 2011, s. 650-653. DOI: 10.1109/INM.2011.5990647. ISBN 978-1-4244-9219-0. Dostupné také z: <http://ieeexplore.ieee.org/document/5990647/>
- [24] PODERMAŇSKI, Tomáš a Matěj GRÉGR. *Deploying IPv6 - practical problems from the campus perspective* [online]. In: . [cit. 2019-11-02].
- [25] MARTIN, Tim. IPv6 Sys Admin Style. In: *SlideShare* [online]. 2016 [cit. 2019-11-02]. Dostupné z: <https://www.slideshare.net/tjmartin2020/ipv6-sysadmins-63071235>
- [26] Cisco SAFE Reference Guide. In: *Cisco* [online]. San Jose, CA, 8 Júl 2018 [cit. 2019-11-02]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_
- [27] SAFE Overview Guide: Threats, Capabilities, and the Security Reference Architecture. In: *Cisco* [online]. Január 2018 [cit. 2019-11-02]. Dostupné z: <https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-overview-guide.pdf>
- [28] JACKSON, Chris. *Network security auditing*. Indianapolis, IN: Cisco Press, 2010. Cisco Press networking technology series. ISBN 978-1-58705-352-8.
- [29] AKIN, Thomas. *Hardening Cisco routers*. Sebastopol: O'Reilly, 2002. ISBN 05-960-0166-5.
- [30] MCMILLAN, Troy. *CCNA security study guide: exam 210-260*. Indianapolis, Indiana: Sybex, a Wiley Brand, 2018. ISBN 978-111-9409-939.
- [31] VYNCKE, Eric a Christopher PAGGEN. *LAN switch security: What hackers know about your switches*. Indianapolis, IN: Cisco Press, 2008. ISBN :978-1-58705-256-9.

- [32] HUCABY, Dave, Steve MCQUERRY, Andrew WHITAKER a Dave HUCABY. *Cisco router configuration handbook*. 2nd ed. Indianapolis, IN: Cisco Press, 2010. ISBN 978-1-58714-116-4.
- [33] SATRAPA, Pavel. *IPv6: internetový protokol verze 6*. 4. aktualizované a rozšířené vydání. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-808-8168-430.
- [34] STALLINGS, William. *Network security essentials: applications and standards*. 4th ed. Boston: Prentice Hall, 2011. ISBN 978-0-13-610805-4.

Zoznam symbolov, veličín a skratiek

Zoznam príloh

A	Zdrojové súbory	27
A.1	Konfiguračné súbory	27
B	Checklist	29

A Zdrojové súbory

A.1 Konfiguračné súbory

B Checklist